

JOSEPH W. PRICE
ALBIN H. GESS
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE
J. RONALD RICHEBOURG

OF COUNSEL
JAMES F. KIRK

PRICE AND GESS

ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pg@pgpatentlaw.com

#2
jc997 U.S. PTO
09/921235
08/02/01

PRIORITY DOCUMENTS

(Japanese Application Nos. 2000-237017; 2001-019267)

Inventor(s): Tomohiko Kitamura

Title: SYSTEM INTEGRATED CIRCUIT

Attorney's
Docket No.: NAK1-BP67

EXPRESS MAIL LABEL NO. E1873069187US
DATE OF DEPOSIT: August 2, 2001

Tomonino Kiti
NAK1-BP67
(JWP)X949)26

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC997 U.S. PTO
NA/AA/...

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日

Date of Application:

2000年 8月 4日

出 願 番 号

Application Number:

特願2000-237017

出 願 人

Applicant(s):

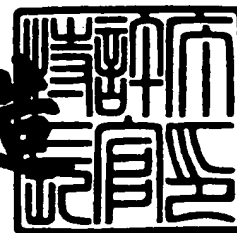
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 6月25日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 2022520331

【提出日】 平成12年 8月 4日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 北村 朋彦

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

特 2 0 0 0 - 2 3 7 0 1 7

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 システム集積回路

【特許請求の範囲】

【請求項 1】 システム集積回路の初期動作の開始を制御する初期状態管理装置と、

前記システム集積回路内部および外部の装置に対しアクセスを行う中央処理装置と、

前記中央処理装置のアクセスに従い外部デバイスにアクセスを行い、また初期状態管理装置からの初期データ読み込み信号に基づき外部デバイスに対しアクセスを行う外部デバイスアクセス制御装置とを有し、

システム集積回路が初期動作を開始する前に外部から初期状態を読み込むことを特徴とするシステム集積回路。

【請求項 2】 請求項 1 のシステム集積回路において、外部デバイスアクセス制御装置に代わり、外部バスアクセス制御装置を有し、システム集積回路が初期動作を開始する前に外部デバイスにデータ出力要求を行うことによりシステム集積回路の初期状態を読み込むことを特徴とするシステム集積回路。

【請求項 3】 請求項 1 のシステム集積回路において、外部デバイスアクセス制御装置に代わり、外部バスアクセス制御装置を有し、システム集積回路が初期動作を開始する前に外部デバイスにアクセスを行うことによりシステム集積回路の初期状態を読み込むことを特徴とする集積回路。

【請求項 4】 請求項 1 から 3 のシステム集積回路において外部から読み込まれたデータをシステム集積回路内の暗号復号装置などのデータ変換装置で変換し、システム集積回路内部に秘密データを保持することを特徴とするシステム集積回路。

【請求項 5】 請求項 4 のシステム集積回路において、データ変換装置の出力する秘密データを元に、外部バス制御装置が外部バスに対してバスをスクランブルして出力することを特徴とするシステム集積回路。

【請求項 6】 請求項 1 から 5 のシステム集積回路において、外部装置からの読み込みを複数回繰り返すことにより、使用する信号線数より多くの初期情報を

読み込むことを特徴とするシステム集積回路。

【請求項 7】 請求項 1 から 6 のシステム集積回路において、システム集積回路が初期動作を開始する前に外部から初期状態を読み込むのではなく、初期動作の開始と同時もしくは開始後に初期状態を読み込み、初期状態を必要とする前に読み込みを完了することを特徴とするシステム集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、システム集積回路内部の初期状態を設定するための手段に関するものである。

【0002】

【従来の技術】

受信したストリームデータを蓄積することができるデジタル放送の受信機は、認証制御等の都合によりシステム集積回路に機器個別の初期状態を設定することが好都合である。システム集積回路において初期状態を設定するためには、その製造段階で値を固定する事で実現可能であるが、そのシステム集積回路を使用した機器個別に異なった初期値を設定することや、機器の製造完了時点で機器個別の認識番号を設定するなどの要望には応えられない。また、初期状態の設定には、設定用のプログラムを実行しシステム集積回路内のレジスタに設定する方法も実現可能であるが、そのプログラムを解析する事により初期設定の状態を外部から観測することが可能となり不正行為が行われる危険がある。

【0003】

【発明が解決しようとする課題】

デジタル放送受信機や有料コンテンツを扱う機器において、各機器を識別するための機器固有情報の設定や、集積回路内部で暗号に使用する秘密データの設定が必要となってきている。しかし、各機器個々に異なった情報を与える必要があり、集積回路に事前に隠蔽しておくことは出来ない。ROMのデータ領域に情報として蓄積し起動時にソフト処理を行い設定を行うことも可能であるが、マイコンの動作をトレースされた場合にその安全性は低下してしまう。外部から初期状態

の設定課程をトレースされず、各機器個別に異なった初期状態設定を可能とするのが本発明の目的である。

【0004】

【課題を解決するための手段】

上記目的を達成するために本発明は、システム集積回路が初期設定値を必要とする前に外部デバイスから初期設定値を読み込むことでシステム集積回路の内部に初期値および秘密データを保持することが可能となる。

【0005】

【発明の実施の形態】

以降、図面を参照しながらLSI内部信号観測手段について説明する。

【0006】

（実施の形態1）

図1は、実施の形態1におけるシステム集積回路の構成を示す図である。図1に示すように本システム集積回路は、初期状態管理装置11と、中央処理装置12と、外部デバイスアクセス制御装置13とを備える。

【0007】

初期状態管理装置11は、システム集積回路内で初期状態を管理し、電源ON若しくはリセット信号を受信すると、中央演算処理装置に動作開始信号を出力する前に、外部デバイスアクセス制御装置13に外部デバイスへのアクセスを行うためのタイミング信号を出力する。外部デバイスアクセス制御装置は、初期状態管理装置からのタイミング信号に基づき外部デバイス14に対しアクセス制御信号を出力し外部デバイスからデータを読み込みシステム集積回路内部の初期値として利用される。この際、初期値は所定のレジスタに保存されるので、特別に不揮発性メモリ等を設ける必要が無い。初期状態管理装置は、前記外部デバイスからの初期データの読み出し終了後、中央演算処理装置に対し動作開始信号を出力し中央演算処理装置は動作を開始する。外部デバイスアクセス制御装置は、中央演算処理装置からの要求に応じて外部デバイスへのアクセスを行う。

【0008】

以上のように本実施例によれば、中央演算処理装置が動作を開始する前に外部

デバイスからシステム集積回路の初期状態を設定することが可能となる。

【0009】

(実施の形態2)

図2は、実施の形態2におけるシステム集積回路の構成を示す図である。図2に示すように本システム集積回路は、初期状態管理装置21と、中央処理装置22と、外部バスアクセス制御装置23を備え、中央処理装置と初期状態管理装置の機能は実施の形態1と共通する。外部バスアクセス制御装置は外部バスを介して複数の機器と接続することができ、外部バスに接続される特定の機器、例えば外部デバイス2(24)に対してアクセス制御信号をバスを介して出力し、同様にバスを介して外部デバイスからデータを読み込む点で実施の形態1と異なる。

【0010】

以上のように本実施の形態によれば、システム集積回路に1個以上の外部デバイスが接続される場合においても、外部デバイスからシステム集積回路の初期状態を設定することが可能となる。

【0011】

(実施の形態3)

図3は、実施の形態3におけるシステム集積回路の構成を示す図である。図3に示すように本システム集積回路は、初期状態管理装置31と、中央処理装置32と、外部バスアクセス制御装置33を備え、中央処理装置32の機能は実施の形態2と共通である。初期状態管理装置31は外部バスアクセス制御装置33を介さずに、直接外部デバイスに接続され、直接アクセス制御信号を伝達する点で実施の形態2と異なる。

【0012】

以上のように本実施例によれば、システム集積回路に1個以上の外部デバイスが接続される場合においても、外部デバイスからシステム集積回路の初期状態を設定することが可能となる。

【0013】

(実施の形態4)

図4は、実施の形態4におけるシステム集積回路の構成を示す図である。図4

に示すように本システム集積回路は、初期状態管理装置41と、中央処理装置42と、外部バスアクセス制御装置43とを備える。初期状態管理装置41は、システム集積回路内で初期状態を管理し、電源ON若しくはリセット信号を受信すると、中央演算処理装置に動作開始信号を出力する前に、外部バスアクセス制御装置43に外部デバイスへのアクセスを行うためのタイミング信号を出力する。外部バスアクセス制御装置は、初期状態管理装置からのタイミング信号に基づき外部デバイスに対し、制御信号バスを介してアクセス制御信号を出力する。外部デバイスはこの信号を受信すると、暗号化データを外部バスアクセス制御装置に対し返信する。外部バスアクセス手段はこれを受信すると暗号復号装置45に出力し、暗号復号装置45はこれを解読して所定のレジスタに復号された秘密データを保存する。

【0014】

以上のように本実施例によれば、システム集積回路の初期状態を設定する際に設定データをバス上で観測することができないため、認証鍵等を隠蔽する際に有効である。

【0015】

(実施の形態5)

図5は、実施の形態5におけるシステム集積回路の構成を示す図である。実施の形態4と異なる点は暗号復号装置55は復号した秘密データを外部バスアクセス制御装置53に返し、外部バスアクセス制御装置はこれをスクランブル鍵として外部バスをスクランブルすることができる点である。

【0016】

以上のように本実施の形態によれば、システム集積回路の外部バスをスクランブルすることが可能となる。

【0017】

なお、実施の形態1から5において初期状態管理装置は初期状態の検出として電源のONやリセット信号の入力を検出として使用するとしたが、これに限定されるものではなく、他の信号を使用しても構わない。また、中央演算処理装置が動作を開始するタイミングとしてシステム集積回路内のリセット信号の解除タイミ

ングを使用しても構わない。また、初期状態を読み込むための外部バスへのアクセスとして外部デバイスへの読み込みシーケンスを専用に出力するのではなく、外部バス制御装置の有する初期値を利用しても構わない。

【 0 0 1 8 】

また、外部デバイスからのデータの読み込みを複数回繰り返すことにより多量の初期情報をシステム集積回路に与えることが可能となる。さらに、中央演算処理装置の動作開始前でなく、同時もしくはその後で初期状態を利用する前に初期状態を読み込んでも構わない。このような場合、初期状態が読み込まれた事を示す情報フラグを設けることで、その初期状態が有効であるかを判断する機構を設ける事が有効になる。

【 0 0 1 9 】

【発明の効果】

以上述べたところから明らかなように、本願発明によるシステム集積回路を用いれば、不揮発性メモリ等の特別な構成を要さず、且つ安全にシステム集積回路の初期状態を設定することができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 にかかるシステム集積回路の構成を示す図

【図 2】

本発明の実施の形態 2 にかかるシステム集積回路の構成を示す図

【図 3】

本発明の実施の形態 3 にかかるシステム集積回路の構成を示す図

【図 4】

本発明の実施の形態 4 にかかるシステム集積回路の構成を示す図

【図 5】

本発明の実施の形態 5 にかかるシステム集積回路の構成を示す図

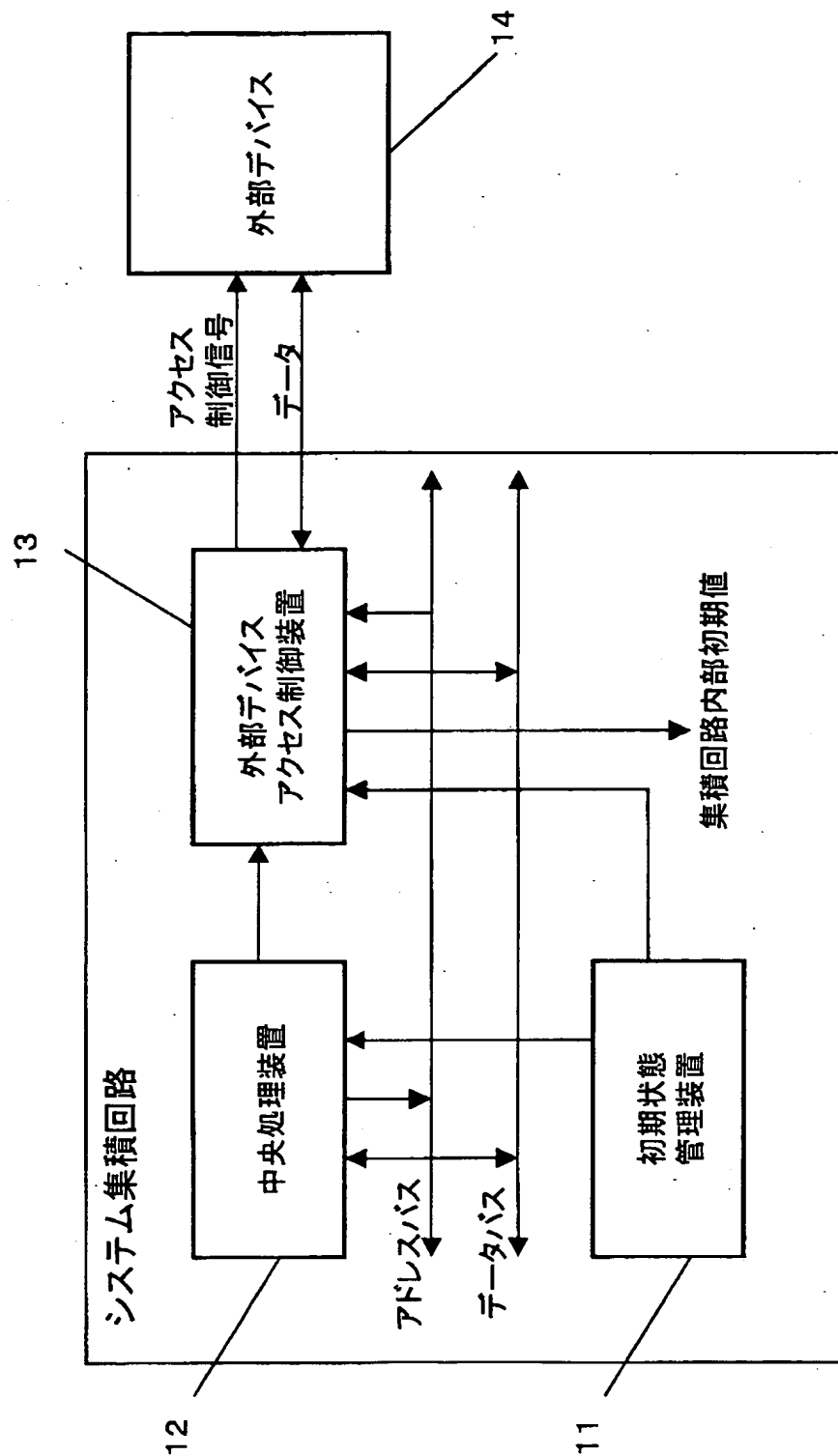
【符号の説明】

- 1 1 初期状態管理装置
- 1 2 中央演算処理装置

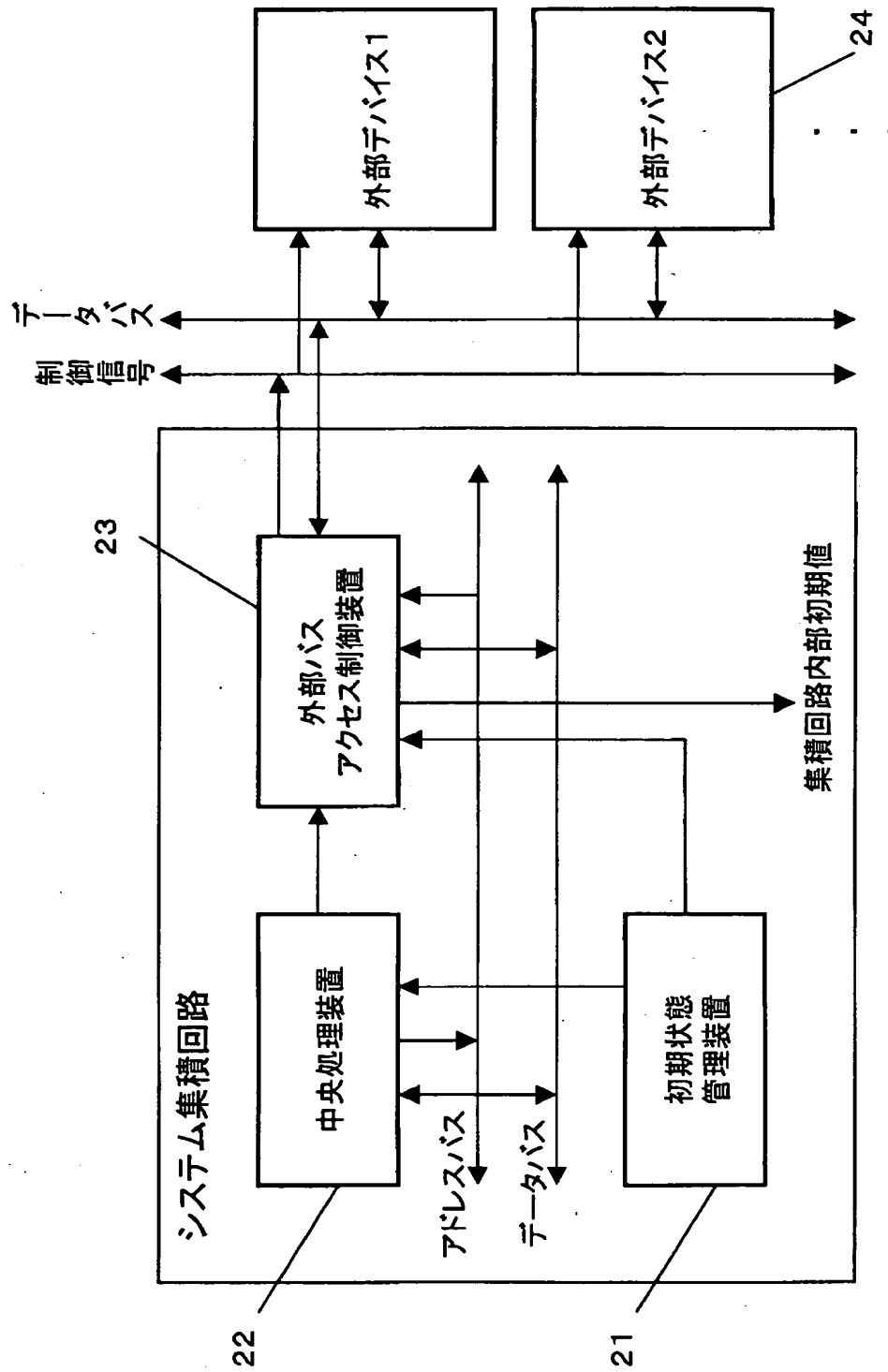
- 1 3 外部デバイスアクセス制御装置
- 1 4 外部デバイス
- 2 1 初期状態管理装置
- 2 2 中央処理装置
- 2 3 外部バスアクセス制御装置
- 2 4 外部デバイス
- 3 1 初期状態管理装置
- 3 2 中央処理装置
- 3 3 外部バスアクセス制御装置
- 3 4 外部デバイス
- 4 1 初期状態管理装置
- 4 2 中央処理装置
- 4 3 外部バスアクセス制御装置
- 4 4 外部デバイス
- 5 1 初期状態管理装置
- 5 2 中央処理装置
- 5 3 外部バスアクセス制御装置
- 5 4 外部デバイス
- 5 5 暗号復号装置

【書類名】 図面

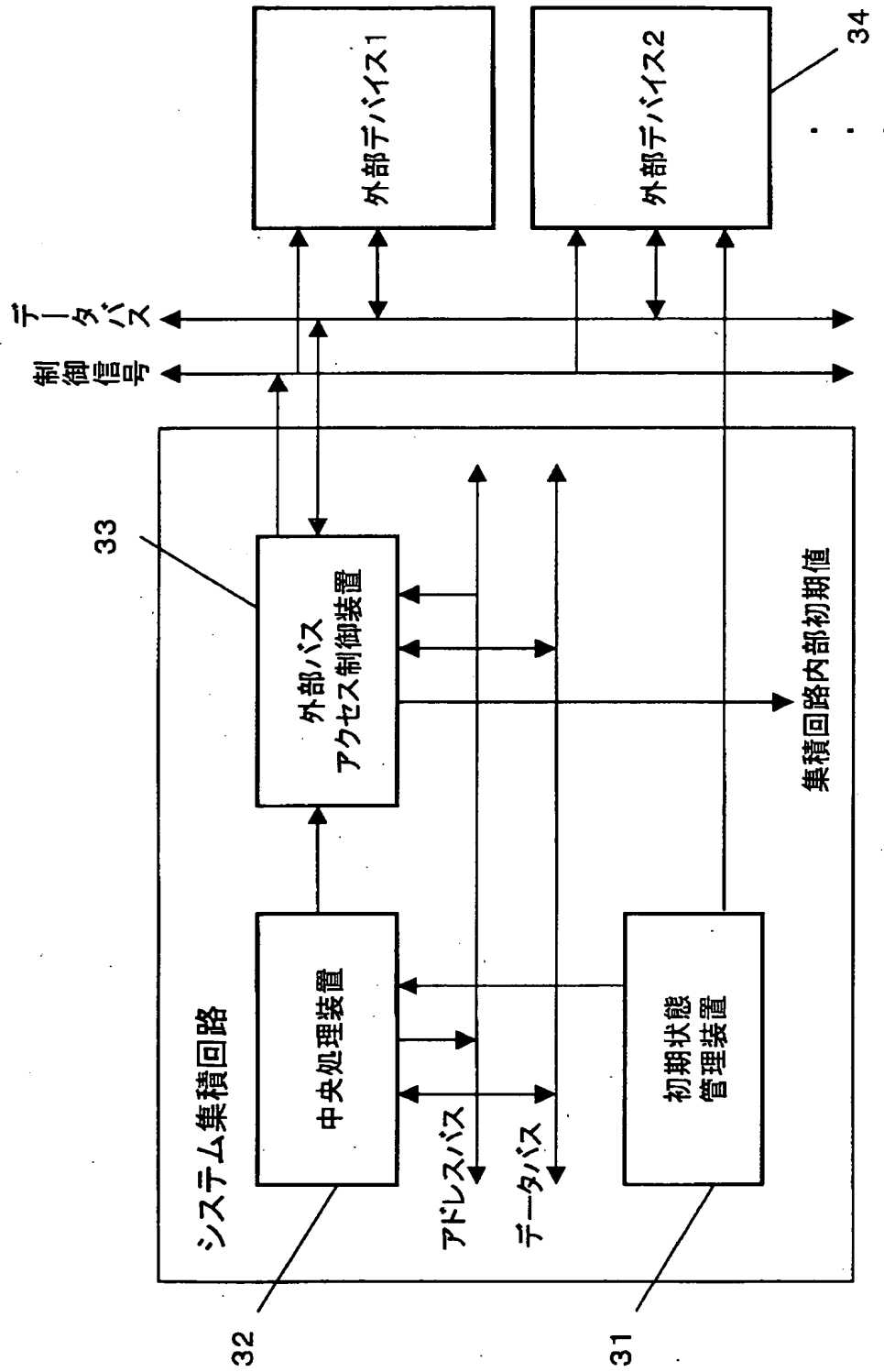
【図 1】



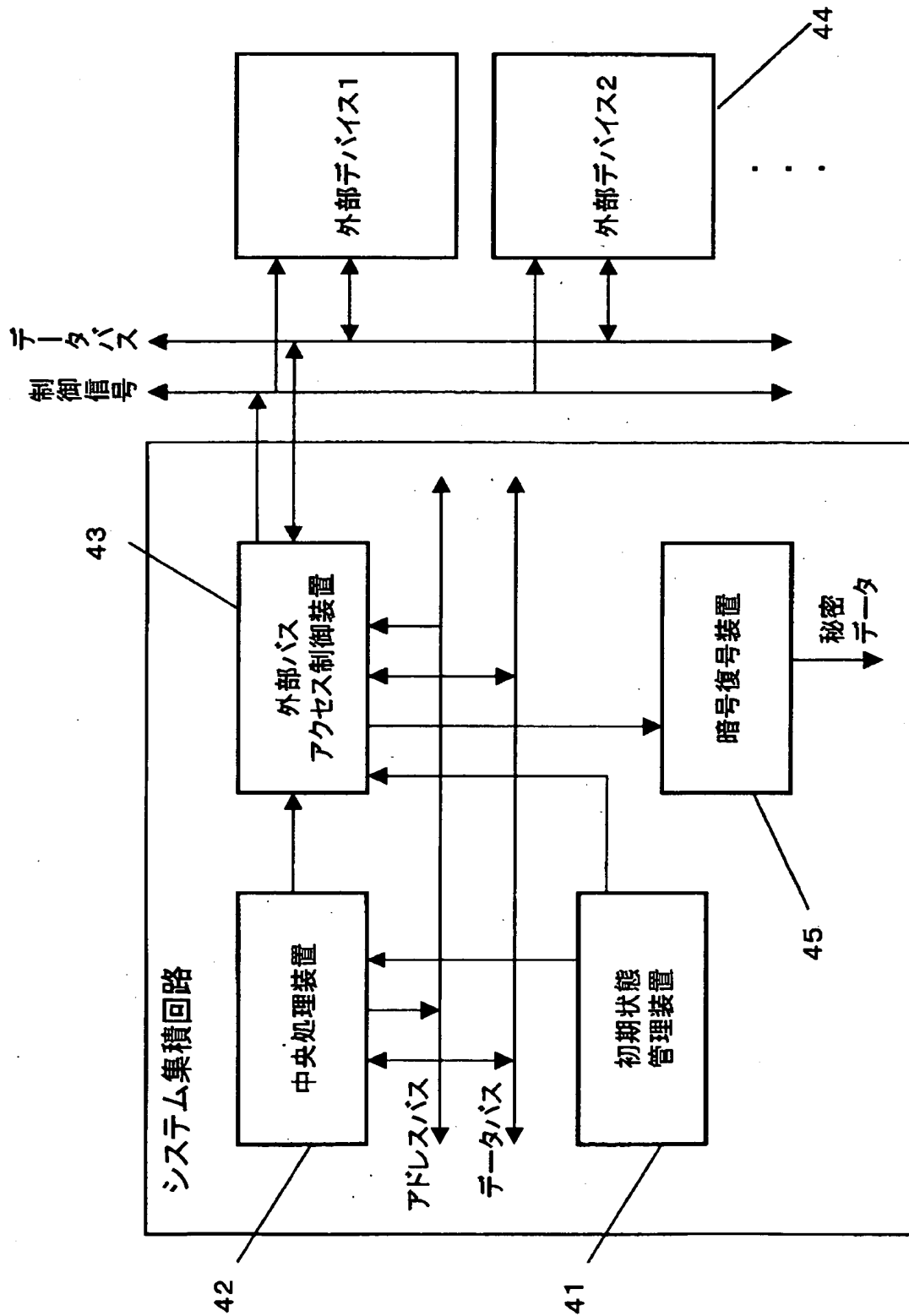
【図 2】



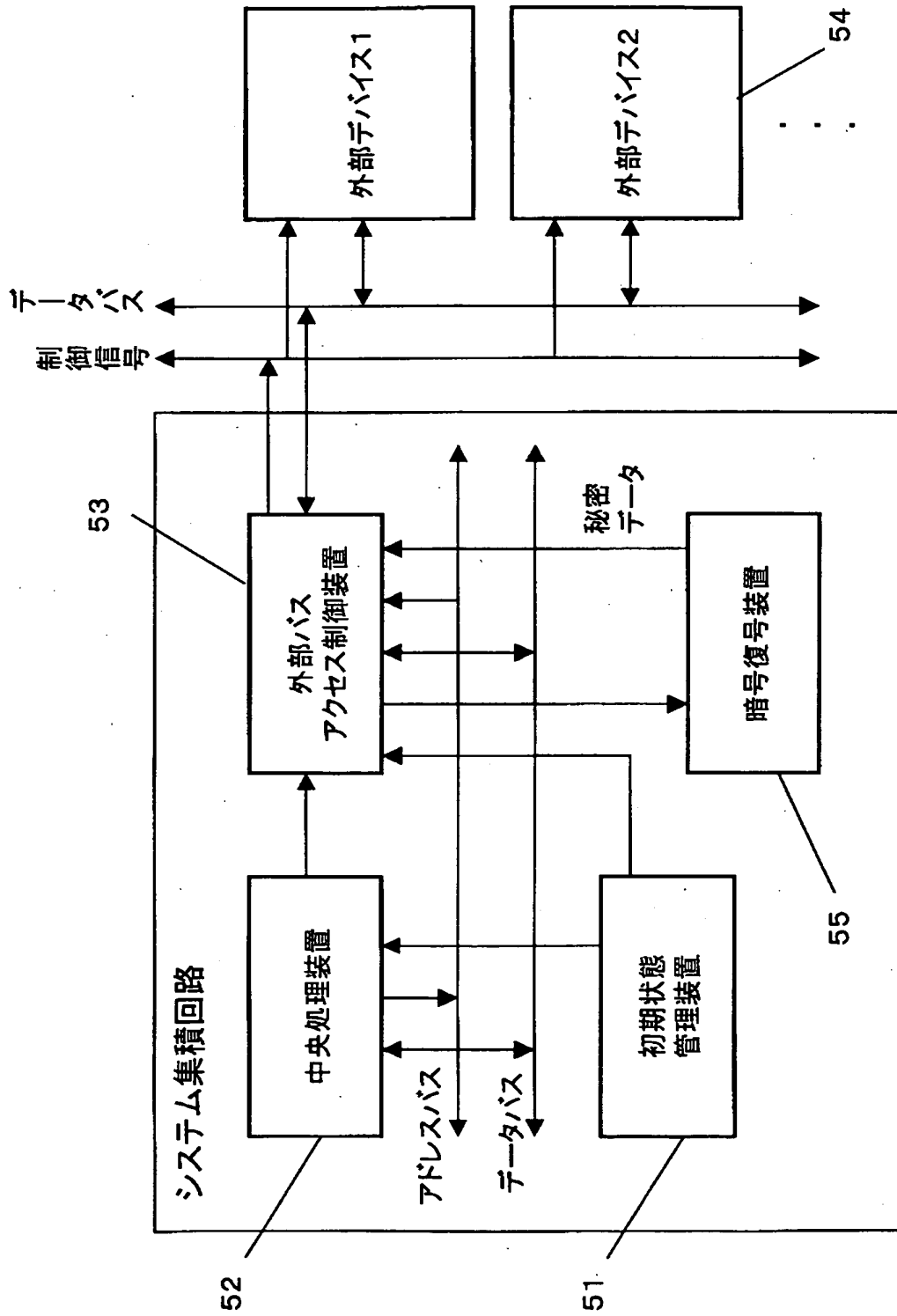
【図3】



【図 4】



【図5】



【書類名】 要約書

【要約】

【課題】 デジタル放送受信機や有料コンテンツを扱う機器において、各機器を識別するための機器固有情報の設定や、集積回路内部で暗号に使用する秘密データの設定が必要となってきた。しかし、各機器個々に異なった情報を与える必要があり、集積回路に事前に隠蔽しておくことは困難である。ROMのデータ領域に情報として蓄積し起動時にソフト処理を行い設定を行うことも可能であるが、マイコンの動作をトレースされた場合にその安全性は低下してしまう。外部から初期状態の設定課程をトレースされず、各機器個別に異なった初期状態設定を可能とするのが本発明の目的である。

【解決手段】 上記目的を達成するために本発明は、システム集積回路が初期状態を使用する前に外部デバイスから初期設定値を読み込むことでシステム集積回路の内部に初期値および秘密データを保持することが可能となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社